Mise en place DMZ

Objectifs de cette séquence d'exercices :

- Expliquer le fonctionnement d'un firewall et de ces règles
- Implémenter des règles de firewall en fonction d'un cahier des charges
- Identifier les principes fondamentaux d'une DMZ.
- Expliquer le fonctionnement d'un proxy et d'un revers proxy.

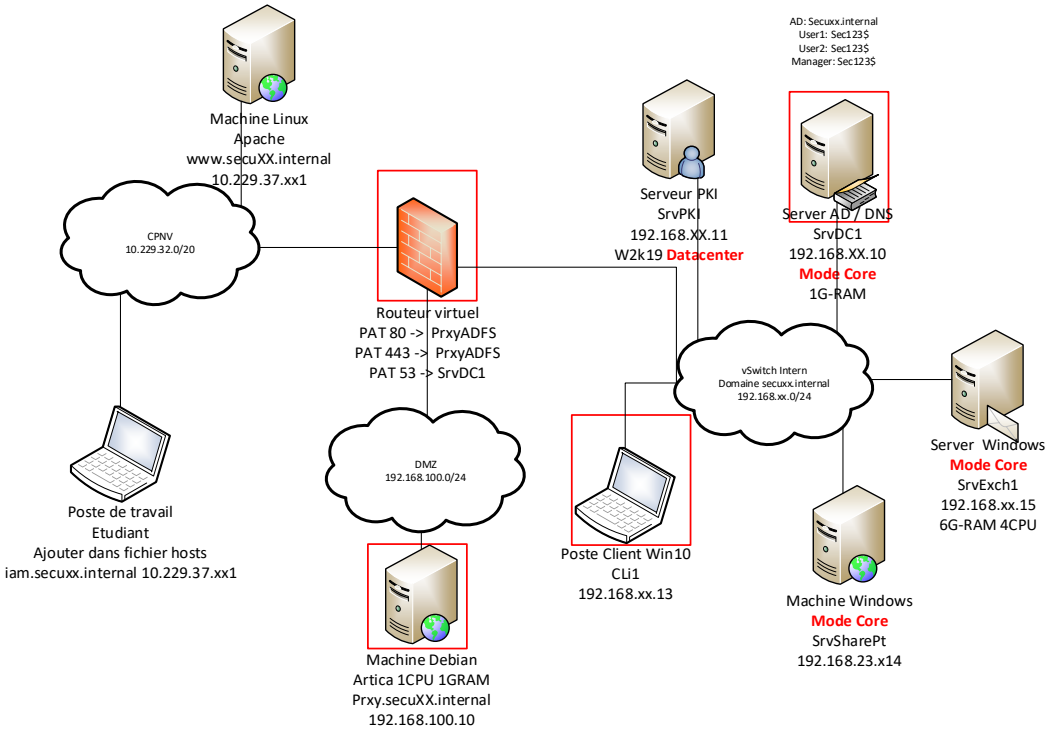
Console à utiliser :

- Outil de management Mikrotik : `winbox.exe`

Documents/fichiers :

- https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work
- https://www.thegeekstuff.com/2011/01/iptables-fundamentals/
- https://wiki.mikrotik.com/wiki/Basic_universal_firewall_script
- https://homenetworkguy.com/how-to/create-basic-dmz-network-opnsense/
- https://www.commentcamarche.net/contents/610-serveur-proxy-et-reverse-proxy
- https://ubuntu.com/server/docs/proxy-servers-squid
- http://articatech.net/download/PROXY-PAC.pdf
- http://articatech.net/download/SSL-PROXY.pdf
- https://www.silicon.fr/5-questions-comprendre-dechiffrement-ssl-100250.html (Inspection SSL)
- https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/26402/preventingcertificate-warnings-ca-signed-certificate

Schéma :
Machines nécessaires pour le module sont entourée en rouge



1 – Analyse infrastructure:

Concept d'un firewall

- Expliquer à quoi servent les tables de NetFilter
- Expliquer à quoi servent les chaines de NetFilter
- En fonction des paramètres par défaut des firewalls définir sous forme explicative quelques règles

Concept d'une DMZ :

- Lister les principes généraux d'une DMZ
- Identifier les flux de l'infrastructure ainsi que leurs directions
- Etudier les différentes infrastructures possibles pour une DMZ

Concept d'un proxy :

- Expliquer le fonctionnement d'un proxy, d'un proxy transparent et revers proxy
- Analyse de divers produit et choix d'un proxy pour la DMZ
- Définir comment déployer la configuration d'un proxy de manière automatique
- Qu'est-ce que c'est une inspection SSL profonde et comment ça marche

2 – Mise en place de la DMZ:

Cahier des charges (10pts):

1. En tant qu'utilisateur du LAN j'aimerai accéder à Internet de manière sécurisée dans le but de ne pas compromettre la sécurité de mon entreprise.

2. En tant qu'utilisateur du LAN j'aimerai que mon navigateur soit configuré de manière automatique au niveau du proxy à utiliser, dans le but de se simplifier la vie.

3. En tant que responsable de la sécurité, j'aimerai que les machines de mon infrastructure puissent communiquer en respectant les principes d'une DMZ, dans le but de sécurisé mon infrastructure contre la compromission d'une ou plusieurs machines. Cette user story sera compléter dans la partie radius.
   Test d'acceptation : Schéma réseau avec les flux, tableau du firewall (source, destination, protocole, action), copie d'écran des règles du firewall

4. En tant que CTO, j'aimerai que les utilisateurs du LAN puissent surfer sur un nombre restreint de sites (www.cpnv.ch, www.vd.ch), pour améliorer leur productivité.

5. En tant que responsable de la sécurité, j'aimerai que le LAN puisse accéder au WAN uniquement à l'aide de ping et protocoles web (https, http), dans le but de protéger l'infrastructure

6. En tant que responsable informatique, je veux que les internautes puissent avoir accès à un site web dans le DMZ qui réponde à http://iam.secuxx.internal, dans le but de par la suite mettre en place un service d'authentification.

Dans la rubrique analyse infrastructure, vous avez choisi un proxy (physique ou logiciel) pour l'implémentation du proxy dans la DMZ, la proposition est d'utiliser squid.
Une note sera attribuée à l'implémentation de l'infrastructure en regard des User Story exprimées. Le temps a disposition pour la mise en place est de 8 périodes.

US	Test	Résultats
1	Accès à Internet, au travers du proxy. Vérifier que ce n'est pas possible d'accès à Internet sans le proxy	
2	Création d'un nouvel utilisateur. Sans configuration manuel du navigateur, l'utilisateur doit passer par le proxy	
3	Schéma des flux autorisé et interdit	
4	Accès à Internet uniquement sur cpnv.ch et vd.ch et on doit avoir un message d'alerte pour tous les autres sites.	
5	Vérification des règles du pare-feu et ping afin de garantir que l'isolation et en place. Test LAN->WAN, WAN->LAN	
6	Règles de pare-feu qui acceptent que http(s) depuis le LAN	
7	Test depuis l'extérieur à l'adresse iam.secuxx.internal qui doit arriver sur une page (peu importe le contenu) du proxy	